CryptoGen Nepal

TECHNICAL PROPOSAL FOR

Phishing Campaigns

MSSP Alert TOP 250

ICT AWARD 2020 STARTUP CATEGORY

EST. 2019

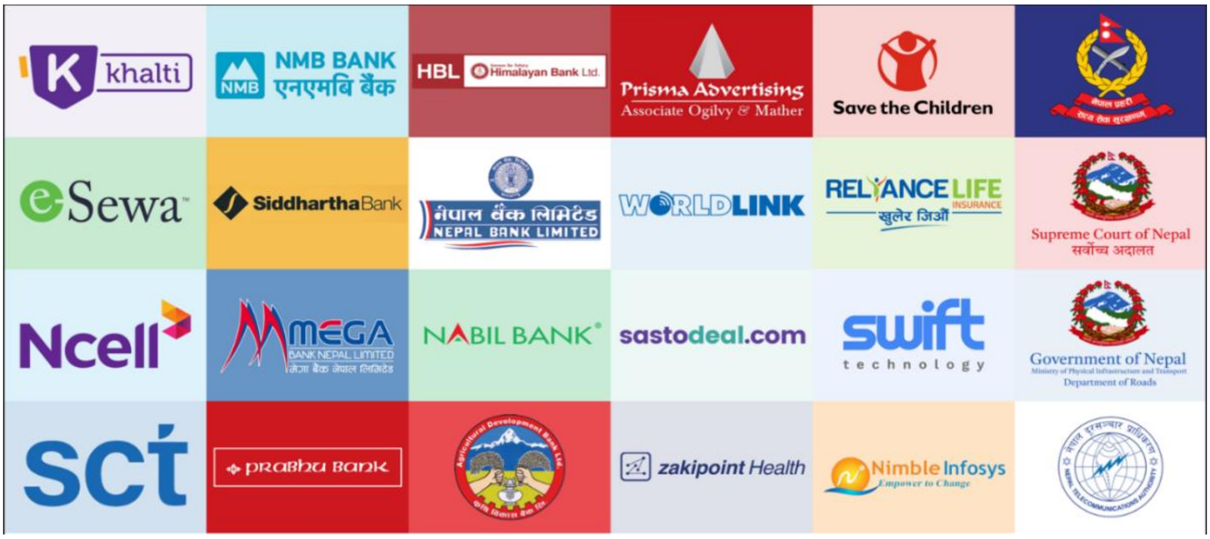
ISO/IEC 27001:2022

Table of Contents

About CryptoGen Nepal

We are a Nepal based Information Security company founded in 2019. We provide professional-grade cybersecurity solutions for all your Information Technology infrastructures. Our team has been demonstrating vulnerability assessment and penetration testing skills using methodologies such as OSSTMM, PTES, NIST SP 800-115, and OWASP. We aim to help companies protect their valuable data from any internal and external threats. We design, implement and support technology solutions with an exclusive focus on achieving our customers' goals through an innovative approach.

Our team consists of industry-experienced professionals and certified resources. We have served several organizations from multiple domains with our broad range of services. Our reaches have been depicted below:



Our team members have been honing their skills to detect and report vulnerabilities in a live environment and have identified vulnerabilities and helped to secure. The below listed companies have recognized our team members for reporting security vulnerabilities and flaws.

We deliver quality service to our customers based on the skills acquired from the few lists of certifications mentioned below. Also, we have set a major milestone of getting compliant with the international standard ISO 27001:2013 for enhancing our ISMS monitoring and assessing the current IT Systems from an Info Security perspective and securing our customer's confidence.

Our Mission

To be the only leading partner in the market to create a safer place free from external threats and risks by delivering the world-class security assessment and solutions.

Our Vision

To create a cyberspace free from threats, risks, and externalities.

Phishing

Phishing is a type of fraud or a social engineering attack in which an attacker poses as a legitimate entity or person through email or other forms of contact. Attackers frequently use phishing emails to distribute malicious URLs or files that can carry out several tasks. Some will take victim's login information or account information. For example, a hacker may send emails requesting account details that appear to be from a legitimate credit card business or financial institution, often implying that there is a problem. Attackers can use the information provided by users when they reply with the required details to access the accounts. Phishing attacks frequently use social networking strategies along with email or other electronic communication channels. Direct messages delivered across social networks and SMS text messages are two examples of techniques. Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- natural disasters (e.g., earthquake, flood)
- epidemics and health scares (e.g., Covid)
- major political elections
- holidays and festivals

Some of the common indicators of phishing attempts are

- **Suspicious sender's address:** The sender's address can be a fake of a real company. By changing or removing a few characters, cybercriminals frequently use an email address that nearly resembles one from a trustworthy organization.

- **Generic greetings and signature:** A generic greeting, such as "Dear Valued Customer" or "Sir/Ma'am," and the absence of contact details in the signature block are clear signs that an email is a phishing attempt. A reputable business would often use your name and offer their contact details.

- **Spoofed hyperlinks and websites:** Any links in the email body that do not correspond to the text that shows when you hover your mouse over them may have been faked. Malicious websites may resemble genuine websites exactly, but the URL may have a different domain or a different spelling (e.g., .com vs. .net). Additionally, to disguise the link's real location, cybercriminals may employ a URL shortening service.

- **Spelling and layout:** Misspellings, uneven formatting, and poor language and sentence structure are other signs of a potential phishing effort. Reputable organizations employ specialized staff to create, confirm, and edit client correspondence.

- **Suspicious attachments:** Malware is frequently spread through unsolicited emails that ask recipients to download and open attachments. To get a user to download or open a file without first carefully reading it, a cybercriminal may create a false feeling of urgency or importance.

Methodology

The following methodologies will be followed to successfully launch the phishing campaign. The cycle can repeat several steps or even numerous times, every step until the attack is detected, stopped, or the attacker is happy with the outcomes, dependent on the nature of the assault and the target.

- **Information Gathering:** It is only natural for most attacks to invest time and attention in this phase. The likelihood of success is dependent on this phase. Techniques of information collection are developed in the framework. Some of the collected information like email and name could be used to identify the attack vector, potential passwords, identify probable responses from different people, refine goals, familiarize with the victim's activity and lifestyle.

- **Delivery:** Various tools and technologies are used in this stage to spoof the sender email as well as to create an email which looks like the domain. The trust between the attacker and the victim is established in this phase. This is crucial since it affects the victim's participation and how much they would disclose or trust the channel. This is because of the relationship that the bogus or bait account we created.

- **Execution:** The platforms used in this project to harvest personally identifiable information (PII) are installed and created in this phase. Such as fake login pages. The platforms maybe any cloned site which asks for the victim's credentials in a certain time to proceed further. After the installation and exploitation, the attacker accounts would end the conversation by leaving the email's hanging without forcing or provoking the target to fall in the trap. This is to avoid making the target realize that they are being attacked. The act must be accepted as a voluntary act and not more.

- **Reporting:** After the previous phases are completed the entire attack is documented for a report. The report includes the entire plan and execution of the campaign as well as the weak points for social engineering in regards of client with the proper remediation and awareness.

Phishing Campaign

A phishing campaign is the behavior of an attacker trying to manipulate one or more individuals for a shared objective, such as credential harvesting, endpoint penetration, or invoking a response.

Cryptogen Nepal provides an annual or onetime phishing campaign to its client with the time interval of every two months repeatedly. Within the campaign various OSINT tools are used to gather the emails, if not provided in the scope. The expertise of Cryptogen Nepal carry out the campaign with intelligence gathering, enticing content along with persistence and patience. The Campaigns are scheduled during the business hours when the targets are working. Additionally, depending on the number of targets, email delivery is staggered over one or more days. Once a campaign is scheduled and delivery is underway, we target to ensure our phishing infrastructure is maintained and ready. This includes both the mail server delivering phishing emails and the web server hosting any phishing websites. After the execution of the phishing mails to the targeted victims, the results are analyzed, and the weak points are noted down to provide a proper remediation, prevention measures as well as session awareness accordingly. The entire campaign is documented in a report and provided to the client to take the necessary action against it.

Timeline

Phase	Tasks	Duration (Days)
Platform Setup	• Server configuration • Domain setup • Mass Mail Service Provider configuration • Other system configurations	1–2
Template Development	• Review client's website for template creation • Monitor upcoming events, festivals or celebrations for contextual relevance • Create phishing email templates	1–2
Pre Simulation Check	• Team alignment and briefing • Identify and address potential troubleshooting issues • Conduct final pre simulation review	1–2
Simulation Launch	• Execute phishing campaign	1–2
Observation & Monitoring	• Monitor campaign performance and user interaction	7
Deliverables	• Prepare and submit detailed campaign report	1–2

Note: Buying a domain is simple in theory but for realistic phishing simulations we must intentionally acquire names that are visually and cognitively indistinguishable from the target, this selection process is deliberate and time consuming. Below are the prioritized domain variation techniques used to maximize deception: *Character omission, Character repeat, Adjacent character swap, Adjacent key replacement, Double replacement, Adjacent key insertion, Missing dot, Strip dashes, Insert dash, Singular/plural, Common misspellings, Vowel swaps, Homophones, Bit-flipping, Homoglyphs/Punycode, Domain prefix, Domain suffix, TLD/SLD swaps, Keyboard layout targeting, Popularity scoring.*

Deliverables

After the campaign, we will be providing the following deliverables:

- Phishing Campaign report mentioning the methodology including technical summary of identified risks, proof of concept, impacts, and possible solutions to remediate those risks along with the debrief trainings. Furthermore, the report will consist of the strong remediation & recommendation of the risks discovered based on the global standard.
  - Technical Summary of identified risks
  - Detailed explanations
  - Scenario Explanations and outcomes

- An Executive Report summarizing the overall, risks, security gaps, and issues with evidence observed. This report depicts the security posture of the organization human assets we assess. Moreover, the report also shows how such issues can affect the business of the organization along with suggestions including best practices to follow for the future. Unlike the technical report, it will be non-tech friendly.

- We will be providing one remote or onsite Brief Presentation to explain the overall findings, measures to prevent those, and possible security services to enhance the security posture of the human assets audited.

Assumptions and Exceptions

- A point of Contact shall be provided for smooth communication and ease (preferably IT Admins) through the campaign.
- It is assumed that organization is utilizing monitoring tool to collect logs. As it is recommended to utilize the monitoring tool for log collection throughout the phishing campaign.
- Except the authorized executive organizations employees should not be aware of the running phishing campaign.
- The Mail ID from which the phishing campaigns are performed should be whitelisted by the client.
- Client needs to provide the list of Email IDs of the employee on the provided Excel format.

Disclaimer

Performance of the above Scope may involve the Parties exchanging/disclosing certain proprietary and confidential information. The confidential and proprietary information means any information and data, whether oral or written, relating to either party's product, tools, strategies, and future products, including but not limited to: licensing practices and fees, research, and development plans, customer lists, marketing, and future business plans, any concepts, opinions, data, schedules, know-how, designs, business, and technical information, customer lists and any documents or record-bearing media which are observed by a Party or disclosed by or transmitted to a Party by the other party.

We agree that Information shall ONLY be used solely in connection with the Subject Matter of this proposal and shall not be disclosed to a third party other than an affiliated company of the receiving party which has agreed, in writing, to be bound by the terms of this Proposal. Where the receiving Party or any of its Representatives shall be under a legal obligation in any administrative or judicial circumstance or by operation of law to disclose any Confidential Information, the receiving Party shall, if possible, give the disclosing Party prompt notice thereof (unless it has a legal obligation to the contrary) so that the disclosing party may seek a protective order or another appropriate remedy. If such protective order is not obtained, the receiving Party and its Representatives shall furnish only that portion of the information that is legally required and shall disclose the Confidential Information in a manner designed to preserve its confidential nature.

Accepting this proposal means each party shall protect Information of the other party using the same degree of care, but no less than a reasonable degree of care, as such party uses to protect its own confidential information. We would like to draw you the attention that you may face the cyberattacks during or before or after the engagement with us. It is your responsibility to protect your assets from any cyber-attacks, incidents, breaches, or vulnerabilities. We will fully use its available preventive and protective measures against the possible scanning and testing activities during the scope outlined above.

OUR SERVICES

Our Services As Information Security Company Includes:

- SECURITY OPERATIONS CENTER
- INFORMATION SECURITY AUDIT
- SWIFT CSP ASSESSMENT
- DARKWEB MONITORING & BRAND PROTECTION
- VULNERABILITY MANAGEMENT
- PENETRATION TESTING
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER CONFIGURATION ASSESSMENT
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING

CryptoGen Nepal

/cryptogennepal
www.cryptogennepal.com
+977-1-4528928
whois@cryptogennepal.com